DATA GOVERNANCE POLICY

1. OBJECTIVE

This Data Governance Policy (the "Policy") aims to establish the regional framework that guides the management, use, protection, quality, and availability of data processed by **Emergent Cold LatAm** ("Emergent Cold," "ECLA," or the "Company"), ensuring that such data is managed in a lawful, secure, accountable, and effective manner, aligned with the Company's strategic objectives and business continuity requirements.

This Policy defines the corporate guidelines for data governance across all regional operations, promoting consistent practices that enable the management of data as a strategic asset, reduce risks associated with data processing, strengthen information reliability, and ensure compliance with applicable laws and regulations in each country regarding privacy, personal data protection, information security, and related sector-specific requirements.

Furthermore, this Policy establishes the regional and local governance structure for the oversight, coordination, and escalation of data governance matters, including the roles and responsibilities applicable to supervisory and control functions, such as Compliance, Technology, Information Security, and other relevant stakeholders. Its purpose is to ensure an appropriate segregation of duties, operational independence in oversight functions, and effective coordination with local data management and processing owners.

The implementation of this Policy enables **Emergent Cold LatAm** to strengthen a comprehensive regional data governance model based on the principles of data quality, availability, transparency, risk mitigation, and continuous improvement throughout the data lifecycle.

2. SCOPE

These guidelines apply to the following:

a. All data generated, received, managed, stored, or used by Emergent Cold LatAm, regardless of its format (physical, digital, or hybrid) or nature. This includes, without limitation, operational, commercial, contractual, logistics, administrative, financial, business continuity, information security, and any

other data necessary for the Company's activities. It also includes all personal data and, where applicable, special categories of personal data processed during business operations.

b. All data processing activities carried out in connection with ECLA's operations, including, by way of example, contact information relating to customers (B2B), consignees, shippers, suppliers, carriers, visitors, employees, job applicants, and any other third party whose data is processed by the Company.

c. All personnel, regardless of their contractual relationship with the Company (including employees, contractors, consultants, and temporary workers), as well as suppliers, service providers, processors, and sub-processors who access, manage, process, or otherwise handle data on behalf of the Company in any country where it operates.

This Policy applies to all facilities, systems, processes, business units, and technology environments involved in the data lifecycle, whether managed directly by the Company or by third parties on its behalf.

3. REGULATORY FRAMEWORK

This Policy is issued and shall be interpreted in accordance with the legal and regulatory frameworks applicable in each country where Emergent Cold LatAm operates, including laws and regulations relating to data governance, personal data protection, information security, cybersecurity, and business continuity, as applicable to the Company's activities.

This Policy is also supported by applicable sector-specific regulatory requirements and by regulations, directives, or guidance issued by competent authorities at the national or regional level whenever such requirements impose specific obligations regarding the collection, use, management, retention, protection, or disclosure of data in connection with the Company's operations.

Furthermore, ECLA adopts internationally recognized principles, best practices, frameworks, and guidelines relating to data governance, risk management, information security, and cybersecurity, applying them in a manner that is proportionate to its operational model and consistent with the legal requirements applicable in each jurisdiction.

This Policy should be read in conjunction with other corporate policies, standards, procedures, and guidelines governing privacy, information security, records management, technology governance, risk management, and related compliance obligations across the region.

Finally, this Policy is integrated with the internal policies, procedures, standards, and guidelines of **Emergent Cold LatAm** relating to personal data protection, information security, incident management, business continuity, and other components of the Company's regional compliance and risk management framework, all of which shall be construed and applied in a complementary manner.

4. DEFINITIONS

For the purposes of this Policy, and without prejudice to the definitions established under applicable laws in each jurisdiction, the following terms shall have the meanings set forth below:

- **Data Governance:** The set of structures, roles, principles, policies, practices, and procedures that guide the management, use, quality, protection, and administration of data throughout its lifecycle, ensuring its responsible use and alignment with corporate objectives.
- **Data Governance Committee (DGC):** The governance body responsible for leading, overseeing, and providing strategic direction regarding data governance guidelines, initiatives, and controls within **Emergent Cold LatAm**.
- **Data Subject Rights:** The rights granted to individuals regarding the processing of their personal data, which may include, as applicable, the rights of access, rectification, updating, erasure, objection, restriction, portability, and any other rights provided under applicable law.
- **Data Subject Rights Management Procedure:** The internal processes and communication channels established by **ECLA** to receive, manage, and respond to requests submitted by data subjects in accordance with applicable legal requirements and corporate policies.
- **Local Data Protection Officer:** The individual designated within each local operation to coordinate the implementation of personal data protection policies and programs, manage local privacy-related risks, support the handling of data requests, and serve as the local liaison with the regional Compliance team and other relevant functions.

- **Regional Data Governance and Protection Function:** The regional team or function responsible for establishing regional policies and standards, overseeing their implementation in each country, providing technical and regulatory support, monitoring compliance, and escalating significant risks or incidents when necessary.
- **Data or Information Asset:** Any information generated, received, managed, stored, processed, or used by the Company, regardless of its format or medium, that has operational, legal, financial, commercial, or strategic value.
- **Data Lifecycle:** The sequence of stages through which data passes during its existence, including its creation or collection, use, storage, sharing, retention, archival, and secure disposal.
- **Data Owner** The business function, department, or individual accountable for the classification, quality, use, and management of a specific dataset, as well as for ensuring that access and processing are performed in accordance with applicable legal, regulatory, and corporate requirements.
- **Data Steward:** The individual designated by the Data Owner to support the day-to-day management of data, including the implementation of data governance controls, monitoring of data quality, and compliance with established standards and procedures.
- **Data Processing:** Any operation or set of operations performed on data, whether by automated or non-automated means, including collection, recording, organization, structuring, storage, adaptation, consultation, use, disclosure, sharing, transfer, alignment, restriction, deletion, or destruction.
- **Personal Data:** Any information relating to an identified or identifiable natural person, either directly or indirectly, in accordance with the definition established under applicable data protection laws.
- **Sensitive Personal Data:** Personal data that, due to its nature, requires enhanced protection under applicable laws, including categories such as health information, biometric data, genetic data, racial or ethnic origin, religious beliefs, political opinions, trade union membership, or other categories recognized by local legislation.
- **Data Processor:** Any natural or legal person, internal or external to the Company, that processes personal data on behalf of **Emergent Cold LatAm** and under its instructions.
- **Data Quality:** The degree to which data is accurate, complete, consistent, reliable, relevant, and up to date for its intended business purpose.
- **Data Classification:** The process of assigning a category or protection level to data based on its sensitivity, criticality, legal requirements, and

business value, with the objective of applying appropriate security and governance controls.

- **Critical Data:** Data whose loss, alteration, disclosure, unauthorized access, or unavailability could significantly impact business operations, business continuity, regulatory compliance, information security, or the commercial interests of Emergent Cold LatAm.
- **Data Flows:** The movement, transfer, or exchange of data between systems, business units, processes, countries, or third parties, including both internal sharing and external transmissions.
- **Authorized Access**: Permission granted to individuals, roles, or systems based on the principles of business need, least privilege, and proportionality, allowing them to access, use, modify, or process data within the scope of their assigned responsibilities.
- **Data Incident:** Any event that compromises, or has the potential to compromise, the confidentiality, integrity, availability, quality, or traceability of data, including unauthorized access, loss, destruction, alteration, corruption, disclosure, or misuse.
- **Data Traceability**: The ability to identify, reconstruct, and monitor the origin, use, modifications, access, transfers, and lifecycle of data through reliable records and audit trails.
- **Anonymization:** The process by which personal identifiers are permanently and irreversibly removed or transformed so that an individual can no longer be identified, directly or indirectly, from the data.
- **Pseudonymization**: A technique that replaces personal identifiers with codes, aliases, or indirect attributes, thereby reducing the exposure of personal data while preserving its usability for authorized purposes.
- **Data Ecosystem**: The collection of processes, systems, platforms, technologies, people, and governance mechanisms that interact to enable the management, protection, sharing, and use of data within Emergent Cold LatAm.

5. GUIDING PRINCIPLES

Data governance at Emergent Cold LatAm shall be based, at a minimum, on the following principles:

a. Lawfulness: All data processing activities must be supported by a valid legal basis and carried out in accordance with applicable legal and regulatory requirements.

b. Purpose Limitation and Compatibility: Data shall be collected and processed for specific, explicit, and legitimate purposes and shall not be used in a manner incompatible with those purposes.

c. Data Minimization and Proportionality: Only the data necessary to fulfill the intended purpose shall be collected, accessed, processed, or retained.

d. Data Quality and Integrity: Data shall be accurate, complete, consistent, and kept up to date to support reliable business operations and decision-making.

e. Confidentiality and Security: Appropriate technical and organizational measures shall be implemented to protect data against unauthorized access, disclosure, alteration, loss, or destruction.

f. Storage Limitation: Data shall be retained only for as long as necessary to fulfill legal, regulatory, operational, or business purposes, and shall thereafter be securely deleted, anonymized, or archived as appropriate.

g. Transparency: Clear and appropriate information regarding data processing activities shall be provided to data subjects and other relevant stakeholders when required.

h. Accountability: Compliance with data governance requirements shall be demonstrable through documented controls, records, evidence, monitoring activities, and oversight mechanisms.

i. Risk-Based Approach: Data governance controls and safeguards shall be designed and implemented based on the level of risk associated with the data processing activity, considering factors such as the nature of the data, volume, sensitivity, operational criticality, exposure, involvement of third parties, and supporting technologies.

6. ROLES AND RESPONSABILITIES:

The effective implementation of Data Governance requires the coordinated participation of multiple roles and organizational structures at both the regional and local levels. Each participant is responsible for carrying out specific functions aimed at ensuring that data is managed, protected, and used in a responsible, secure, and business-oriented manner.

The following roles and responsibilities establish the baseline governance framework to be applied consistently across all regional operations, without prejudice to additional requirements that may apply under local laws and regulations.

6.1. Compliance Committee

The Compliance Committee is the governing body responsible for providing oversight and strategic direction for Data Governance. Its responsibilities include:

- Approving this Policy and any subsequent updates.
- Establishing strategic guidelines, prioritizing initiatives, and resolving conflicts relating to data access, use, and ownership across business functions.
- Ensuring alignment between this Policy, the Personal Information Management Program (PIMP), and related procedures, including lawful bases for processing, retention and disposal requirements, incident management, and third-party risk management.
- Periodically reviewing risks associated with data processing activities and requiring remediation or improvement plans where necessary.
- Coordinating with Information Security, Compliance, and the Data Protection Officer(s) (DPOs) to ensure the implementation of appropriate controls, monitoring activities, and supporting evidence of compliance.

6.2. Local Data Protection Officer (Country-Level Role)

ECLA shall designate a Local Data Protection Officer within each country's operation to coordinate the effective implementation of this Policy and the data protection program at the local level. The Local Data Protection Officer shall operate with appropriate functional independence and shall have access to the information, resources, and support necessary to perform their responsibilities, including:

- Monitoring, interpreting, and advising on applicable data protection laws, regulations, guidance, and best practices within their jurisdiction, and informing the relevant operational areas and the Regional Compliance team of any developments or requirements that may impact the processing of personal data.

- Overseeing compliance with this Policy, the Personal Information Management Program (PIMP), and related procedures, including those regarding lawful bases for processing, retention, incident management, and third-party data processing arrangements, identifying gaps and proposing corrective actions where appropriate.
- Maintaining and validating compliance documentation, including records, evidence, registers, matrices, procedures, and guidance materials, and supporting the preparation of data protection impact assessments when required.
- Coordinating and managing the data subject rights request process, including the receipt, assessment, response, escalation, and recordkeeping of requests submitted by data subjects.
- Serving as the primary local liaison between business functions and regional oversight teams on personal data protection matters and supporting the implementation of regional initiatives, controls, and remediation actions.
- Coordinate, together with Information Security and Compliance, the management of incidents and breaches involving personal data, ensuring appropriate traceability, documentation, and preservation of evidence.
- Deliver and promote periodic data protection training and awareness activities for employees and teams involved in data processing activities.
- Serve as the primary operational point of contact for internal inquiries relating to personal data processing, while maintaining appropriate confidentiality and professional discretion.

Mandatory Escalation: When any of the following situations arise: (i) complex or sensitive data subject requests, (ii) regulatory inspections, investigations, or requests from competent authorities, (iii) significant matters involving lawful bases for processing, international data transfers, data processors or sub-processors, incidents, or high-risk decisions, the Local Data Protection Officer shall consult and coordinate with the Regional Data Protection Officer before issuing a final response or making a final determination. Where urgency prevents prior coordination, the Regional Data Protection Officer shall be informed immediately thereafter.

6.3. Regional Data Governance and Data Protection Lead

Emergent Cold LatAm shall designate a Regional Data Governance and Data Protection Lead responsible for providing regional oversight, direction, and governance regarding data governance and personal data protection matters.

This role shall operate with an appropriate degree of functional independence to issue guidance, recommendations, and reports, and shall report directly to the Board of Directors or the equivalent governing body designated by the Company.

Responsibilities include:

- Establishing regional policies and standards relating to data governance, personal data protection, risk management, and integration with applicable corporate policies, ensuring a consistent approach across the region.
- Requesting and reviewing periodic reports from Local Data Protection Officers, including compliance metrics, risk assessments, incidents, data breaches, audit results, implementation of controls, and any other relevant supporting evidence.
- Assessing and issuing guidance on critical matters escalated by Local Data Protection Officers, including regulatory inspections, significant incidents, data protection impact assessments, high-risk processing activities, decisions involving vendors and third parties, and any matter requiring regional direction. The role shall coordinate with Information Security, Technology, and Compliance teams to ensure consistent responses to regional regulatory requirements.
- Presenting periodic reports to the Board of Directors or the designated governing body, covering the regional compliance status, key risks, incidents, metrics, breaches, mitigation measures, and improvement plans, without prejudice to extraordinary reporting when warranted by the severity of a particular matter.

7. INTEGRATION WITH THE CORPORATE COMPLIANCE PROGRAM

These guidelines form part of the Company's Corporate Compliance Program and are integrated with the applicable corporate policies, standards, and procedures relating to data governance, personal data protection, information security, cybersecurity, business continuity, and other components of the Company's internal control framework.

Compliance with this Policy shall be considered within the Company's risk identification, assessment, and mitigation processes, as well as within the audit, monitoring, and control activities established under the regional governance framework. Failure to comply with the provisions of this Policy may result in

corrective, contractual, disciplinary, or other measures in accordance with Company policies and applicable laws.

Updates and modifications resulting from legal, regulatory, technological, operational, or organizational changes shall be incorporated in a timely manner. Updated versions shall be communicated to the relevant stakeholders and reflected in applicable supporting policies, standards, and procedures.

8. EFFECTIVE DATE AND REVIEW

This Policy shall become effective upon its approval by the Emergent Cold LatAm Compliance Committee and shall remain in force until amended, replaced, or revoked by the Committee.

The Compliance Committee shall conduct a periodic review of this Policy at least every two years, or more frequently when required due to legal, regulatory, technological, strategic, or operational changes. Such review shall consider regulatory developments in the countries where the Company operates, evolving corporate practices, risks associated with data processing activities, and findings from audits, assessments, and monitoring activities.

Any updates to this Policy shall be communicated to all relevant stakeholders and reflected, where appropriate, in the related procedures, standards, guidelines, and supporting governance documentation.